Kasra Ahmadi, Ph.D Candidate.

Tampa, FL, 33617 | E-mail: ahmadi1@usf.edu, Mobile: 8136142640 | Personal webpage: https://kasraahmadi.github.io/
LinkedIn: https://www.linkedin.com/in/kasra-ahmadii | GitHub: https://github.com/KasraAhmadi | Google Scholar

Education

1. University of South Florida, Tampa; **Ph.D. in Computer Science**; Jan 2022 to Sep 2025; GPA: 3.93/4
2. Amirkabir University of Technology, Tehran; M.Sc. in Information Technology; Sep 2018 to Jul 2021.
3. Isfahan University of Technology**,** Isfahan; B.Sc. in Computer Science; Sep 2012 to Jul 2017.

Skills

- **Data** AWS Glue, Airflow, Kafka, Kinesis, PowerBI, Postgres, MongoDB
- **ML** Pytorch, Pandas, Numpy, Flower, Scikit-learn, Huggingface 😊
- **Programming** Python, C, C++, Verilog, Typescript, Node.js, Java, JavaScript, Bash, QT, QML, SQL
- **Cloud** Lambda, Step functions, S3, EC2, DynamoDB, Aurora, IAM, API Gateway, CloudFormation
- **IoT** Vitis, ARM Cortex-M4, FPGA, Stm32, Raspberry Pi, AVR, Arduino
- **Others** Linux, Git, Docker, Jira, GraphQL, Rest API, Wireshark, Selenium, Postman, Webservice

Work Experience

- **University of South Florida,** Tampa, US — Jan 2022 - Present
  Research Assistant
  - Researching algorithm level error detection schemes for **Number Theoretic Transform (NTT)** utilized in **Kyber** and **Dilithium,** NIST selected **Post-Quantum Cryptography (PQC)** schemes.
  - Researching, simulating, and implementing **algorithm-level error detection** schemes for classical cryptosystems such as the **Montgomery Ladder** and **Window method for ECSM**.
  - Researching fine-tuning large language models (**LLMs**) using **Federated Learning**, while ensuring privacy protection through the implementation of **differential privacy (DP)**.
  - Performance assessment of Post-Quantum Cryptography schemes on **FPGAs**, **ARM**, and **Embedded Linux**.
  - Work under National Science Foundation (NSF) Grant # 1801488;
  - Teaching assistant of graduated Cryptography, Operating Systems, Network Lab, and System Design Lab.

- **Transparency Wise**, St.Petersburg, US — May 2024 - Aug 2024
  Technical Team Lead, Intern
  - Managed a team of 3 software engineers and 2 designers to develop a **recommender system** for nutrient recommendations tailored to various growth stages of corn and soybeans to achieve high yield farming practices.
  - Implemented an **event-driven** architecture utilizing **Lambda functions**, **Step Functions**, **Event Bridge**, **SES**, and **API Gateway** to promote loose coupling and **scalability**. Additionally, leveraged **AWS Glue** as **ETL** tool for processing laboratory reports to support the recommender model.

- **Paar Lift,** Tehran, Iran — Jan 2019 - Apr 2020
  Data Scientist
  - Analyzed optimal floor levels for elevators at specific times to reduce passenger wait times using machine learning, such as **Logistic Regression** and **KNN**. Utilized data-driven approaches to enhance elevator efficiency and passenger experience.
  - Establishing a connection between Raspberry Pi embedded boards and elevators through the CAN bus protocol for the real-time data transfer of elevators to a Linux-powered **IoT**.
  - Building **ETL** pipelines by using Apache airflow to extract, ingest, and load elevator traffic data to an **OLAP** storage.
  - Performing **Data visualization**, **big data analytics,** and **statistical modeling** on elevators traffic data.
  - We decreased hotels passengers' waiting time by 27%, equating to a time savings of 11 seconds per passenger. Project's demo.

- **Dodong,** Isfahan**,** Iran — May 2017 - Dec 2019
  Technical Team Lead
  - Managed a team of 4 software engineers to launch of a realtor platform. Performed as Backend and Devops engineer to build backend utilizing Node.js**,** MongoDB, MySql, and Nginx.
  - Task assigning and project management using **agile framework**, **scrum**, and **Jira**.

Publications

1. **Efficient Error Detection Schemes for ECSM Window Method Benchmarked on FPGAs**
   K. Ahmadi, S. Aghapour, MM Kermani, R. Azarderakhsh
   IEEE Transactions on Very Large Scale Integration (VLSI) System, vol. 32, no. 3, pp. 592-596, March 2024.
2. **PUF-Kyber: Design of a PUF-Based Kyber Architecture Benchmarked on Diverse ARM Processors**
   S Aghapour, **K Ahmadi,** M Anastasova, MM Kermani, R Azarderakhsh
   IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, early access, 2024.
3. **Efficient Error Detection Cryptographic Architectures Benchmarked on FPGAs for Montgomery Ladder**
   K. Ahmadi, S. Aghapour, MM Kermani, R. Azarderakhsh
   IEEE Transactions on Very Large Scale Integration (VLSI) System, early access, 2024.
4. **A P2P File Sharing Marketplace based on Blockchain and IPFS with Dispute Resolution Mechanism**
   K. Ahmadi, M Esmaili, S Khorsandi
   2023 IEEE International Conference on Artificial Intelligence, Blockchain, and Internet of Things (AIBThings), 2023.
5. **Efficient Algorithm Level Error Detection for Number-Theoretic Transform Assessed on FPGAs and ARM**
   K. Ahmadi, S. Aghapour, MM Kermani, and R. Azarderakhsh,
   ACM Transactions on Embedded Computing Systems, under review, 2024**.**
6. **Error Detection Schemes for τ-NAF Conversion within Koblitz Curves Benchmarked on Various ARM Processors**
   K. Ahmadi, S. Aghapour, MM Kermani, and R. Azarderakhsh,
   IEEE Transactions on Circuits and Systems I, under review, 2024.
7. **Efficient Fault Detection Architectures for Modular Exponentiation Targeting Cryptographic Applications Benchmarked on FPGAs**
   S. Aghapour, **K. Ahmadi**, M. Mozaffari Kermani and R. Azarderakhsh,
   IEEE Transactions on Circuits and Systems II, under review, 2024.
8. **PUF-Dilithium: Design of a PUF-Based Dilithium Architecture Benchmarked on ARM Processors**
   S. Aghapour, **K. Ahmadi**, MM Kermani and R. Azarderakhsh
   ACM Transactions on Embedded Computing Systems, under review, 2024.
9. **Partial Recomputation Fault Detection Architecture for Multiple-precision Montgomery Modular Multiplication on FPGA**
   S. Aghapour, **K. Ahmadi**, MM Kermani, and R. Azarderakhsh,
   IEEE Transactions on Very LargeScale Integration (VLSI) Systems, under review, 2024.

Certifications

- **AWS Certified Solutions Architect - Associate**, View Certification (Dec 2023)
- Deep Neural Networks with PyTorch, View Certificate (Oct 2024)
- Intro to Federated Learning, View Certificate (Oct 2024)
- Artificial Intelligence Privacy and Convenience, View Certificate (Aug 2024)
- Federated Fine-tuning of LLMs with Private Data, View Certificate (Aug 2024)
- ETL and Data Pipelines with Shell, Airflow and Kafka, View Certificate (Jan 2024)
- Divide and Conquer, Sorting and Searching, and Randomized Algorithms, View Certificate (Oct 2023)

Projects

- **Distributed File Sharing Market Based on Blockchain**
  Deployed a web3 application for a file-sharing marketplace, leveraging the IPFS and Ethereum smart contracts.
- **Secure Microcontrollers Remote Programmer**
  Developed and designed a **QT/QML** application along with a server API using Node.js to enable the programming of Microchip microcontrollers remotely while preserving the company's hex files confidentiality.
- **GPS Car Tracker**
  Utilized **STM32** and ArduinoIDE for the hardware implementation. Additionally, Node.js was employed for the server API.
- **Android Game published on Google Play**
  Designed and developed an online Trivia Android game (Footxam) by using **Java** and **Node.js**.

Services

- Mentor at REU Site: Cryptography and Coding Theory at the University of South Florida (Summer, 2023)
  NSF award: 2244488
- Conducted peer review for **15** manuscripts from "Transactions on Embedded Computing Systems", "IEEE Transactions on Circuits and Systems I: Regular Papers", and "IEEE Transactions on Very Large Scale Integration (VLSI) Systems".
- Speaker at Great American Teach-In (Winter, 2023)